UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,721	12/15/2005	Sheau Bao Ng	US030223US	8499

65913 7590 09/03/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
ARCHER, CHRISTOPHER B	

ART UNIT	PAPER NUMBER
4148	

NOTIFICATION DATE	DELIVERY MODE
09/03/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/560,721	**Applicant(s)** NG ET AL.	
	Examiner CHRISTOPHER B. ARCHER	**Art Unit** 4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 December 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-11_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-11_ is/are rejected.

7)☒ Claim(s) _6_ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _15 December 2005_ is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _12/15/2005_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/560,721 filed on 12/15/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: Figure 2, reference number 150. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required

corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The second half of Claim 10 appears to have inadvertently switched the "first portion" and "second portion" of the memory. The claim was examined as if it read: "The storage module of claim 6, wherein: The information stored in the second portion includes a private key (144) that can be used to decrypt content stored in the first portion of the memory; the storage module further comprises a data decrypter (146) for decrypting data that is stored in the ~~second~~ **first** portion of memory using the private key that is stored in the ~~first~~ **second** portion of the memory." Please correct or clarify this claim.

Claim Objections

5. Claim 6 is objected to because of the following informalities: Claim 6, line 2 recites "if", which appears to be a misspelling of the word "in". Appropriate correction is required.

6. Claim 10 is objected to because of the following informalities: Neither the previous claims, nor the specifications refer to a private key that is stored in the first section of the memory that is required to access data in the second portion of the memory. Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dreifus (US Patent No. 4,575,621) (hereafter referred to as Dreifus), in view of Morishita (US Patent No. 6,839,837 B1) (hereafter referred to as Morishita).

Regarding claim 1, Dreifus teaches "detecting unauthorized use of the storage module;" as **[column 3, lines 23-24 and column 5, lines 1-5 and 34-37, show means for detecting abnormal conditions and unauthorized use of the device],** "preventing access to the information in the second portion after the unauthorized use is detected;" as **[column 3, lines 24-25, show means for disabling the device in response to unauthorized use or abnormal conditions]** and "providing a power source for the detecting and preventing of access, access also being prevented if the power source fails" as **[column 12, lines 15-23, and column 12, lines 50-55 show a battery powered system that will prevent access to sensitive data when power fluctuations or failures are detected]**, but fails to expressly disclose "A method, comprising: providing multiple portions of memory in a storage module, the portions including a first portion for containing content and a second portion containing information that must be accessed in order to access content stored in the first portion;".

However, Morishita teaches "A method, comprising: providing multiple portions of memory in a storage module, the portions including a first portion for containing content and a second portion containing information that must be accessed in order to access content stored in the first portion;" as **[column 2, lines 37-42, show that in an information storage device, keys and secret information are stored in separate means; column 3, lines 7-9, show that these storage means may be separately constructed]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of Morishita into Dreifus' as both are analogous art from the same field of endeavor of storage and prevention of access to sensitive data.

The ordinary skilled person would have been motivated to apply the teaching of Morishita into Dreifus' system, since Morishita's invention adds a clear-cut separation between sensitive data and the cryptographic means necessary to access said data.

Regarding claim 6, Dreifus teaches "access control means (128) for preventing access to content stored in the first portion of memory without accessing information stored if the second portion of memory; means (130) for detecting unauthorized use of the storage module;" as **[column 3, lines 23-24, show any means for detecting abnormal conditions in the device],** "protection means (132) for preventing further access to the information stored in the second portion of the memory after unauthorized use is detected;" **[column 3, lines 24-25, show means for disabling the device in response to unauthorized use or abnormal conditions]**, and "a power source (134) for operating the detecting means and protection means, the protection means also preventing further access to the information stored in the second portion of the memory after the power source fails" as **[column 12, lines 15-23, and column 12, lines 50-55 show a battery powered system that will prevent access to sensitive data when power fluctuations or failures are detected]**.

Morishita teaches "A storage module comprising: multiple portions of memory including a first portion (122) and a second portion (124) of the memory; access control means (128) for preventing access to content stored in the first portion of the memory without accessing information stored in the second portion of the memory;" as **[column 2, lines 37-42, show that in an information storage device, keys and secret information are stored in separate means; column 3, lines 7-9, show that these storage means may be separately constructed]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of Morishita into Dreifus' as both are analogous art from the same field of endeavor of storage and prevention of access to sensitive data.

The ordinary skilled person would have been motivated to apply the teaching of Morishita into Dreifus' system, since Morishita's invention adds a clear-cut separation between sensitive data and the cryptographic means necessary to access said data.

Regarding claim 10, Morishita further teaches "The storage module of claim 6, wherein: The information stored in the second portion includes a private key (144) that can be used to decrypt content stored in the first portion of the memory; the storage module further comprises a data decrypter (146) for decrypting data that is stored in the second portion of the memory using the private key that is stored in the first portion of the memory" as **[column 4, lines 27-32, discloses a decrypting device and a cryptosystem key that are required to decrypt the secret data that is stored in a separate portion of the module. Morishita figure 1 clearly displays this configuration]**.

8. Claims 2, 4, 5, 8, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dreifus in view of Morishita, and further in view of the Federal Information Processing Standards 140-2: Security Requirements for Cryptographic Modules (hereafter referred to as FIPS).

Regarding claim 2, Dreifus and Morishita teach "The method of claim 1", but fail to expressly disclose "wherein access to the information in the second portion is prevented by blank erasing the information in the second portion when unauthorized access is detected."

However, FIPS teaches "wherein access to the information in the second portion is prevented by blank erasing the information in the second portion when unauthorized access is detected" as **[FIPS page 8, 'tamper response' and 'zeroization' show that**

when tampering is detected, the minimum action taken is the zeroization (altering or deleting) of plaintext keys and Critical Security Parameters].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of FIPS into Dreifus' as both are analogous art from the same field of endeavor of storage and prevention of access to sensitive data.

The ordinary skilled person would have been motivated to apply the teaching of FIPS into Dreifus' system since the invention provides an additional detecting means as well as a means of protecting against further access to sensitive data when tampering has occurred.

Regarding claim 4, FIPS further teaches "The method of claim 1, wherein detecting unauthorized use includes detecting unauthorized opening of an enclosure of the storage module" as **[FIPS page 22, security level 3, shows that the device is considered compromised when a door is opened or a cover is removed]**.

Regarding claim 5, FIPS further teaches "The method of claim 1, wherein detecting unauthorized use includes detecting unauthorized opening of an enclosure of a device containing the storage module" as **[FIPS page 22, security level 3, shows that the device is considered compromised when a door is opened or a cover is removed]**.

Regarding claim 8, FIPS further teaches “The storage module of claim 6, wherein: unauthorized use includes unauthorized opening of an enclosure (140) of the storage module; and the detecting means monitors the integrity of an enclosure of the storage module and the protecting means blank erases the information stored in the second portion of the memory when unauthorized opening of the enclosure of the storage module is detected” as **[page 22, security level 3, shows that the device will ‘zeroize’ all plaintext secret and private keys and Critical Security Parameters when a door is opened or a cover is removed]**.

Regarding claim 9, FIPS further teaches “The storage module of claim 6, wherein: unauthorized use includes unauthorized opening of an enclosure (142) of a device containing the storage module; and the detecting means monitors the integrity of an enclosure of the device and the protecting means blank erases the information stored in the second portion of the memory when unauthorized opening of the enclosure of the device is detected” as **[page 22, security level 3, shows that the device will ‘zeroize’ all plaintext secret and private keys and Critical Security Parameters when a door is opened or a cover is removed]**.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dreifus in view of Morishita, and further in view of Kaish (US Patent No. 4,494,114) hereafter referred to as Kaish.

Regarding claim 3, Dreifus and Morishita teach "The method of claim 1," but fail to expressly disclose "wherein detecting of unauthorized use includes detecting unauthorized disconnection of the storage module from a device that uses the storage module."

However, Kaish teaches "wherein detecting of unauthorized use includes detecting unauthorized disconnection of the storage module from a device that uses the storage module" as **[column 3, lines 50-58, show that removal of equipment from its normal authorized operating location is considered a disabling event, upon which the device is rendered inoperable]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of Kaish into Dreifus' as both are analogous art from the same field of endeavor of storage and prevention of access to sensitive data.

The ordinary skilled person would have been motivated to apply the teachings of Kaish into Dreifus' because Kaish offers the additional unauthorized disconnection of a storage module to the unauthorized access conditions mentioned in Morishita and Dreifus.

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dreifus in view of Morishita, and further in view of FIPS, and further in view of Kaish (US Patent No. 4,494,114) hereafter referred to as Kaish.

Regarding claim 7, FIPS, Morishita, and Dreifus teach "The storage module of claim 6," but fail to expressly disclose "wherein: unauthorized use includes unauthorized disconnection of the storage module from a device that uses the storage module; and the detecting means monitors a connection (136) between the storage module and the device that uses the storage module and the protecting means blank erases the information stored in the second portion of the memory when unauthorized disconnection of the storage module from the device is detected."

However, Kaish teaches "wherein: unauthorized use includes unauthorized disconnection of the storage module from a device that uses the storage module; and the detecting means monitors a connection (136) between the storage module and the device that uses the storage module and the protecting means blank erases the information stored in the second portion of the memory when unauthorized disconnection of the storage module from the device is detected" as **[column 3, lines 50-58, show that removal of equipment from its normal authorized operating location is considered a disabling event, upon which the device is rendered inoperable]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of Kaish into Dreifus' as both analogous art from the same field of endeavor of storage and prevention of access to sensitive data.

The ordinary skilled person would have been motivated to apply the teachings of Kaish into Dreifus' because Kaish offers the additional unauthorized disconnection of a storage module to the unauthorized access conditions mentioned in Morishita and Dreifus.

11. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dreifus in view of Morishita, and further in view of Martin et al. (US Patent No. 5,412,791) hereafter referred to as Martin et al.

Regarding claim 11, Morishita, and Dreifus teach “The storage module of claim 6,” but fail to expressly disclose “wherein the information stored in the second portion of the memory includes a table of contents that is necessary to play the content stored in the first portion of the memory."

However, Martin et al. teaches “wherein the information stored in the second portion of the memory includes a table of contents that is necessary to play the content stored in the first portion of the memory" as **[column 6, lines 51-66, and column 7 lines 19-20, show IFS units and disk drives that contain file directory information that is necessary to access the information in the data storage modules]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the teaching of Martin et al. into Dreifus’ as both analogous art from the same field of endeavor

The ordinary person in the art would have been motivated to apply the teachings of Martin et al. into Dreifus because it adds a directory that must be used to locate and access data in the storage module.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571)270-7308. The examiner can normally be reached on M-F 7:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148

/CHRISTOPHER B ARCHER/
Examiner, Art Unit 4148